FlipIt

Simon Forest Baptiste Lefebvre Vincent Vidal

March 29, 2013

Abstract

Ideal cryptography systems are based on a secret, a key, however advanced Persistent Threat (APT) have undermined secure protocols. *FlipIt* [1], [2] is a recent two-player game between an attacker and defender. It provides a simple and elegant framework to formalize their interactions and allows the description of pratical threats.

We propose a variant of FlipIt, a two-player game where players compete to control a shared ressource. Players can move at any given time, taking control of the ressource. However the identity of the player controlling the ressource is not revealed until a player actually moves. We consider that the average move rate by player is bounded, the number of moves made by player up to an including time can not be greater than a constant times this time.

Describe here the structure of this article.

Describe here the results of this article.

1 Formal Definition and Notation

This section gives a formal definition of the variant of FlipIt.

Players There are two players identified with 0 and 1. Keep the game symetric between the two players will be useful for our studies.

Time The game begins at time $t = 0$ and continues indefinitely. It is viewed as being continuous.

Game state $C(t)$ denotes the current player controlling the ressource at time t, $C(t)$ is either 0 or 1.

2 Playing periodically

Describe here the playing periodically study.

References

[1] R. L. Rivest, *Illegitimi non carborundum*, Invited keynote talk given at CRYPTO 2011, August 15, 2011.

[2] M.van Dijk, A. Juels, A. Oprea, and R. L. Rivest, *FlipIt: The Game of "Stealthy Takeover"*, To appear in Journal of Cryptology, 2012.

[3] K. D. Bowers, M. van Dijk, R. Griffin, A. Juels, A. Oprea, R. L. Rivest, and N. Triandopoulos, *Defending against the Unknown Enemy: Applying FlipIt to System Security*, GameSec, 2012.